NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPLEMENTING A FACIAL RECOGNITION SYSTEM TO IMPROVE ACCESSIBILITY AND INCREASE UTILIZATION OF ENTRY CONTROL POINTS AT MILITARY INSTALLATIONS

by

Kristopher Walker

June 2011

Thesis Advisor:	Eugene Paulo
Second Reader:	Deborah Goshorn

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE				*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY ***(Leave blank)***		**2. REPORT DATE** June 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Implementing a Facial Recognition System to Improve Accessibility and Increase Utilization of Entry Control Points at Military Installations				**5. FUNDING NUMBERS**
6. AUTHOR(S) Kristopher Walker				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000				**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number N/A.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited				**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Most military installations utilize an entry control point that is inefficient, time consuming, and manpower intensive. Unfortunately, as a result of the current inefficiency, traffic congestion has become a nuisance for many service members, as well as government employees.

Directive Type Memorandum (DTM) 09-012, "Interim Policy Guidance DoD Physical Access Control" distributed by the Undersecretary of the Navy states that biometric access to military installations shall be implemented when feasible. This thesis addresses the capability gap for an automated entry control point that increases throughput without sacrificing security. Application of the Systems Engineering process, concept of operations, functional and physical architectures provide a general solution that fills the identified capability gap. Additionally, this thesis provides a proof-of-concept prototype solution by means of simulation and modeling.

14. SUBJECT TERMS			**15. NUMBER OF PAGES** 61
Systems Engineering, Facial Recognition, License Plate Recognition, Entry Control System			**16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

IMPLEMENTING A FACIAL RECOGNITION SYSTEM TO IMPROVE ACCESSIBILITY AND INCREASE UTILIZATION OF ENTRY CONTROL POINTS AT MILITARY INSTALLATIONS

Kristopher Walker
Lieutenant, United States Navy
B.A., San Diego State University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2011

Author: Kristopher Walker

Approved by: Eugene Paulo
Thesis Advisor

Deborah Goshorn
Second Reader

Clifford Whitcomb
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Most military installations utilize an entry control point that is inefficient, time consuming, and manpower intensive. Unfortunately, as a result of the current inefficiency, traffic congestion has become a nuisance for many service members as well as government employees.

Directive Type Memorandum (DTM) 09-012, "Interim Policy Guidance DoD Physical Access Control" distributed by the Undersecretary of the Navy states that biometric access to military installations shall be implemented when feasible. This thesis addresses the capability gap for an automated entry control point that increases throughput without sacrificing security. Application of the Systems Engineering process, concept of operations, functional and physical architectures provide a general solution that fills the identified capability gap. Additionally, this thesis provides a proof-of-concept prototype solution by means of simulation and modeling.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AoA	Analysis of Alternatives
C2	Command and Control
CAC	Common Access Card
CONOPS	Concept of Operations
COTS	Commercial-Off-the-Shelf
DIPR	Detect, Identify, Predict, and React
DoD	Department of Defense
DTM	Directive Type Memorandum
ECP	Entry Control Point
ECS	Entry Control System
ESD	External Systems Diagram
GOTS	Government-Off-the-Shelf
GUI	Graphical User Interface
KPP	Key Performance Parameters
MOP	Measures of Performance
NCSE	Network-Centric Systems Engineering
NPS	Naval Postgraduate School
PACS	Physical Access Control System
SoS	System of Systems
SWAP	Size, Weight, and Power
TOC	Total Ownership Cost
UGV	Unmanned Ground Vehicle
VBIED	Vehicle Borne Improvised Explosive Device

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Currently, access to U.S. Navy and most other DoD facilities requires 100% identification check. This requirement implies that a security guard will check for proper identification from the person as well as proper identification for the vehicle entering the installation. This means that cars must have current DoD registration stickers (Form 2220) and drivers must present their DoD Common Access Cards (CAC). Without both of these identification sources, entry is not permitted. This means of identification verification is redundant, time consuming, and manpower intensive.

This thesis designs and recommends a generalized solution based on a Systems Engineering approach in order to address the current problems associated with entry control points at military installations. This thesis starts with the identification of the problem, determines a concept of operations, and defines various requirements. From these requirements, both functional and physical architectures are developed in order to bring form to function.

First presented is the functional architecture that ensures that the requirements are met by a function of the generic system. Each function from the hierarchy is then decomposed into data flow diagrams that ensure data is shared seamlessly between the various functions. Qualitative value models are presented in order to ensure that the functions have a means of being measured. This measured evaluation will provide success and failure criteria.

Next, the physical architectures are presented. Once the baseline system has been properly defined and a general physical architecture exists, this thesis explores the option for alternative functional hierarchies based on the enhanced ECP functional hierarchy. A license plate recognition software program that can be bought off the shelf is explored and defined in order to define the capabilities and limitations of the system. The facial recognition software is based off of the previous work conducted at the Naval Postgraduate School under the “Watchman” project.

Utilizing both the license plate and facial recognition systems are defined in the proof of concept in order to determine configurations that will be chosen for simulation and modeling. A discrete event simulation is used to model three alternatives to the ECP system. The baseline system which contains two manned kiosks, a fully automated system, and an integrated manual and auto system is ultimately chosen for modeling. Of these systems, the model shows that the fully automated system decreases the need for manpower and increases throughput, which ultimately relieves the traffic congestion caused by the baseline system.

Further research is required, providing valid cost benefit evaluation as well as a detailed risk analysis. Additionally, this thesis focuses on accessibility to the base and not security, as that aspect needs to be more fully examined. Finally, the technology presented needs to be further tested for integration feasibility as well as concerns regarding maintainability, availability, and reliability.

To conclude, this thesis provides a concept, requirements, functional and physical architectures to a proposed solution in order to increase throughput and reduce manning requirements for entry control points located at military installations. This thesis uses the Systems Engineering approach to identifying a capability gap and then defines the requirements for an enhanced ECP system.

ACKNOWLEDGMENTS

The author would like to thank Professor Paulo for his devoted time and guidance during the writing of this thesis. Additionally, the author would like to thank Professor Deborah Goshorn for the inspiration and support for this thesis throughout the writing process. Thank you to my family for their unconditional support during this journey of education.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Prior to September 11, 2001, security was more relaxed at many military installations. There were often multiple entry gates that had minimal to no manning requirements. Vehicles were permitted access to bases without much verification. A current Department of Defense (DoD) vehicle registration sticker (DD Form 2220) could suffice for access. Of course, all of this changed after the terrorist attacks that occurred on 9/11. Security was heightened and base vulnerability assessments were conducted to determine if possible weaknesses could be isolated. Restricting access to military installations became a top priority for protecting government assets. There is a tradeoff that comes with this increased security; at the time, increased security required more manning and more time spent conducting these increased security operations. Some of these tradeoffs resulted in increased traffic delays and the necessity for entry control point reconstruction and modification for enhanced security measures.

There is now an opportunity for streamlining the overall process for gaining access to military installations without sacrificing current security requirements. This thesis examines the possibility for facial recognition software to be implemented into military installation entry control points in order to increase throughput, reduce manning requirements, and enhance overall security. The potential benefit to the implementation of this system is to reduce the cost of manning access gates and the amount of waiting time for personnel to access base installations.

B. THE CURRENT MILITARY INSTALLATION ACCESS PROCESS

Currently, access to U.S. Navy and most other DoD facilities requires 100% identification check. This means that cars must have current DoD registration stickers and drivers present their DoD Common Access Cards (CAC), a process that is somewhat redundant and possibly unnecessary. There has been significant talk about eliminating the DoD stickers that employees have on their cars, trucks, and motorcycles. Directive Type Memorandum (DTM) 09-012, “Interim Policy Guidance DoD Physical Access

Control" states the minimum standards for gaining access to military installations no longer requires the use of DD Form 2220 for establishing "trusted agents." DTM 09-012 does not state that DD Form 2220 is an acceptable means of establishing identity to gain access to military installations. Another touted problem with overt vehicle stickers is the possibility that they could provide a "target of opportunity" to a possible terrorist due to their government affiliation. Additionally, when a car gets sold by a service member, the sticker is not necessarily scraped off, which means that the vehicle may still be authorized to gain access to the military installations. The current purpose of the sticker is to provide a secondary identification to the associated base security that a vehicle registered to the DoD employee is driven by a trusted agent that has provided proof of insurance and valid identification, thus deserves the privilege to drive on military installations. This is a redundant check since all military installations require 100% identification check, which is accomplished using the CAC card that each government employee must carry.

One problem of the current DoD sticker program is the database that contains the names and associated vehicles is often outdated and inaccurate. Another problem is that it is time consuming to verify identification at the entry gates of these bases. Not only must the guard at the gate correctly verify and validate an identification card, he must also check that the vehicle DoD sticker is current with the correct military installation and that the date of expiration has not passed. In a post 9/11 enhanced security, "do-more-with-less-era," we must find ways to automate and increase efficiency. Facial recognition software and efficient database management could help eliminate and or reduce the associated problems with the current system.

Having all service members and civilian employees registered into a centralized database that is integrated with facial recognition software that could then be automated at an entry control point within a military installation could eliminate the need for increased security (i.e., increased manning and associated security measures). The increased security could be embedded into the access software. One of the major problems that fleet concentration areas experience is traffic delays in the morning for government employees accessing the bases. If one or two lanes were dedicated to

completely or even semi–automation it could reduce traffic congestion significantly. DoD stickers would be eliminated and security could actually be increased if this sort of automation were implemented.

C. BIOMETRIC IMPLEMENTATION

Biometric authentication being integrated into military installations has been authorized. In accordance with DTM 09-012 (Under Secretary of Defense, 2009), installations will purchase electronic Physical Access Control Systems (PACS) that will provide the capability to electronically authenticate personnel credentials. Additionally, the PACS "shall provide the capability to take, store, and forward to guard stations a facial image and/or digital photograph obtained during registration to perform visual match of the person presenting the credential." (DTM). Basically, once a person registers with the Pass/ID office, has their picture taken, shows proof of vehicle ownership and insurance details, this person is then entered into the central or regional database.

A person could access the military installation using an automated lane that utilizes facial recognition matched with the Pass/ID database records. The vehicle license plate is then captured in order to match the driver to the vehicle. Once the plates and facial recognition matched, authorization to access the base would be established. If any problems were identified such as facial recognition was not matched such as the probability of correct recognition was below a set threshold or the vehicle did not match what the database contained, the person and vehicle would be diverted to a manned control point for further investigation. Several questions arise here concerning the need to cross-check vehicles and their registration status: Do vehicles need to be registered to the person driving in order to be considered accessible to military installations? Or, do we just need to verify that the person alone can be sufficient to gain access? Is security truly enhanced by establishing vehicle registration to a particular government employee? All of these questions should be considered for this type of analysis.

D. SYSTEMS ENGINEERING OVERVIEW

This thesis will propose a generic solution for a problem associated with maintaining high security levels at military entry control points (ECP) by applying a

Systems Engineering approach. This approach will introduce a concept, external systems diagram, requirements, and associated functional/physical architectures. A system that provides autonomous entry control capability that corresponds to the derived requirements is proposed. Finally, a proof-of-concept will be shown in order to demonstrate the feasibility and potential benefit of this entry control system (ECS).

A Systems Engineering process analysis can be utilized for this particular problem in order to provide a possible solution to the inherent problems associated with increased security requirements, demand for right-sized manning, and efficient vehicle throughput. This thesis proposes the use of the Systems Engineering "Vee" process model to propose a solution to the aforementioned problem. The "Vee" model identifies the needs and requirements followed by functional decomposition of the identified requirements (Blanchard and Fabrycky, 2006).

In order to accomplish a detailed analysis, an Extend Sim model is used that shows assumed queuing rates for different scenarios. A current scenario is provided given various threat levels, which are compared with the standard operating procedures that are currently in place.

A fully automated entry control point may never be attained and that is not my intent. Instead, incremental implementation could be a better approach for the current problem. My approach here is to show that security can be enhanced with less people by using proven technology that exists today.

E. THESIS OUTLINE

An overview for each chapter is presented below. Each chapter supports the previous chapter through applying the Systems Engineering process.

1. Chapter II: Systems Engineering Process Model

This chapter provides a background and discussion on the application of the Systems Engineering process model to this particular topic. The Systems Engineering "Vee" process model is used as a roadmap for architecture design associated with the proposed system.

2. Chapter III: Functional Architecture

This chapter presents diagrams as well as the functional architectures that were created utilizing the System Engineering processes identified in Chapter II. Included in this chapter is the Concept of Operations and identified requirements. This chapter lays the foundation that develops the proof of concept system in Chapter V. Specifically, this chapter includes a general functional hierarchy for the ECS, Data Flow Decompositions, and the enhanced ECS functional hierarchy.

3. Chapter IV: Physical Architecture

This chapter presents the general physical architecture associated with the entry control point system. Alternative generation is explained in this chapter. Also, a traceability matrix, alternative physical hierarchies, and the proof of concept are all included within this chapter. Finally, brief descriptions of both license plate recognition and facial recognition are contained in this chapter as well.

4. Chapter V: System Simulation and Analysis

This chapter presents a proposed solution derived from a Naval Postgraduate School (NPS) project named Watchman. The Watchman project contained various scenarios that demonstrated facial recognition software enhancements that could be utilized to develop a semi-automated personnel and vehicle entry system. Additionally, an appropriate discrete event simulation model is built using Extend Sim to execute the proposed architectures and generate simple scenarios. This chapter then evaluates the models in order to recommend the ideal future ECS for military installations.

5. Chapter VI: Conclusion and Summary

This final chapter summarizes the recommendation for the new automated entry control point from Chapter IV and the possible future research for full automation for entry to military installations. This chapter reviews the need and concept for the proposed system and the benefits associated with this system. Additionally, lessons learned from the prototype proof of concept will be applied and analyzed for further refinement.

II. SYSTEMS ENGINEERING PROCESS MODEL

A. SYSTEMS ENGINEERING PROCESS

In order for new and upgraded systems to be cost-effective and efficient, the systems engineering process should be used as a basis for implementation. Simply stated, System Engineering is about doing the right thing right the first time (Forzberg, Mooz, and Cotterman, 2000). Systems Engineering is defined by the U.S. Department of Defense Regulation as an approach to translate operational needs and requirements into operationally suitable blocks of systems. The approach shall consist of a top-down, iterative process of requirements analysis, functional analysis and allocation, design synthesis and verification, and system analysis and control. Systems Engineering principles shall influence the balance between performance, risk, cost, and schedule (U.S. Department of Defense Regulation 5000.2R, 2002). We can conclude from this definition that Systems Engineering is a process that is meant to look at multiple aspects of system acquisition in order to reduce Total Ownership Cost (TOC) with respect to risk and trade-off analysis as presented to the various stakeholders. The ultimate goal here is to increase efficiency while maximizing return on investment.

B. SYSTEMS ENGINEERING PROCESS MODEL

The Systems Engineering process model that will be utilized in this thesis is the Vee model. The process model will act as a baseline for major milestones within the proposed system in order to bring it from concept to implementation. Figure 1 shows a phase-by-phase representation of the desired process model. The basic steps in the systems engineering process is iterative in nature, providing a top-down definition of the system, and then proceeding down to the subsystem level. On completion, the system is defined in functional terms known as “whats.” These “whats” are then translated into “hows” through the iterative process of functional partitioning, requirements allocation, and trade-off analysis. This defines the initial requirements of the system architecture, which is the left side of the Vee (Blanchard and Fabrycky, 2006). The design of the system is complete at the bottom of the Vee. The right side of the Vee is used for

integrating, testing, and verification of the system. Validation occurs throughout these steps in order to ensure that the stakeholder's needs and requirements are being met throughout the process.

This thesis focuses strictly in the region of the Vee in the upper left corner, as it represents a further feasibility study and initial concept exploration without considering important aspects such as cost and risk. Concept and feasibility studies are conducted to begin the preliminary steps in order to decide if a new system needs to be built, an existing capability can fill the identified gap, or an upgrade to an existing system can supplement the need.

A capability gap was identified when DTM 09-012 was issued. It stated that biometric recognition shall be implemented at military installations (Under Secretary of Defense, 2009). Since this need has been identified, a concept of operations can now be created. The concept of operations provides a means to scope and bound the recognized need. Facial recognition coupled with license plate database management is a feasible technology that could fill this identified need. This system concept is identified in Chapter IV.

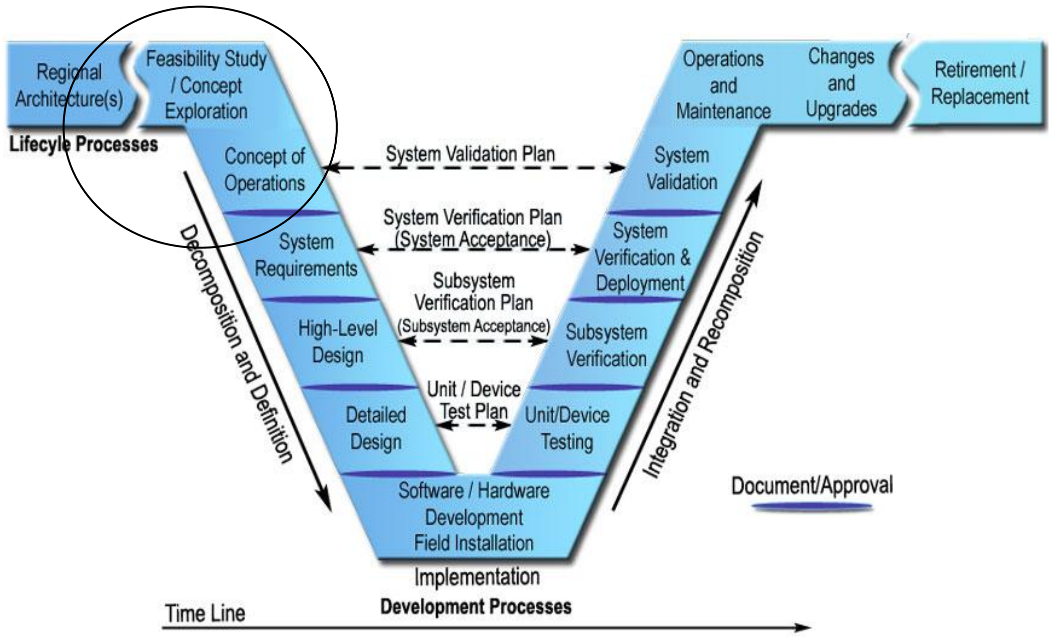

Figure 1. Systems Engineering Vee Model With Focus on Feasibility Study and Concept Exploration (From Department of Transportation, 2011)

THIS PAGE INTENTIONALLY LEFT BLANK

III. FUNCTIONAL ARCHITECTURE

The overall systems architecture is comprised of a set of architectural views. While there are several different systems architectural models available, such as the Department of Defense Architectural Framework (DoDAF), the systems architectural model used in this research is based on Buede (2000). His model consists of three architecture views, which are functional, physical and operational architecture. The overall systems architecture described below includes a functional, physical, and operational architectural component.

The functional architecture narrows the scope of the problem to an enhanced, or automated, system for entry control. Functions and subfunctions within the functional hierarchy reflect emphasis on automated systems. Nevertheless, the systems analysis described in Chapter V includes the current baseline alternative that has very little automation.

A. REQUIREMENTS

The following are implied requirements for the automated ECS, which are derived from experience and intuition as well as discussion with advisory team:

- Detect license plates and conduct facial recognition
- Provide an updatable database with registered users
- Provide a Command and Control capability for decision makers and analysts
- Utilize an alert system for system anomalies
- Provide enhanced security for increased threat conditions
- Minimize manning requirements based on current allocations
- Maximize the vehicle throughput in morning conditions while minimizing the time a vehicle is held in the queue (greater than 2000 vehicles)
- Maximize the security for Entry Control Points at military installations

B. FUNCTIONAL HIERARCHY

1. Top-Level Functions

A functional architecture is a top-level view that establishes the functions in order to meet the overall goal of the system. This simple list of functions establishes a framework for the sub-functions to be derived.

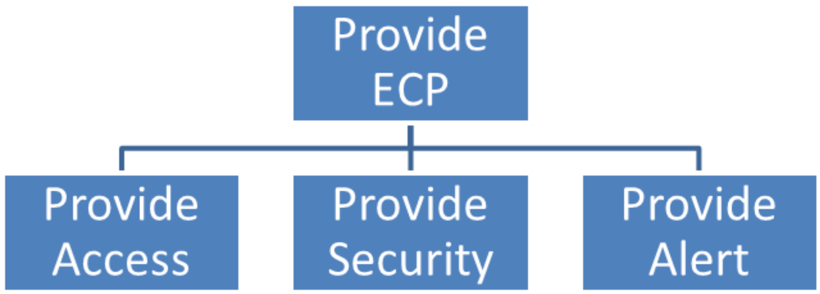

Figure 2. Top Level Functional Hierarchy for ECS

From Figure 2, we see three major functions that comprise the overall ECS Function: Provide Access, Provide Security, and Provide Alert.

The provide access function enables a vehicle to enter the military installation. There may be multiple entry control points leading into the base depending on the size and capability of associated base. Traditionally, a vehicle will be stopped and queried by a physical guard. Multiple guards may be called upon to inspect vehicles and their occupants.

The provide security function deals with varying degrees of security embedded with the ECS. This could include increased guards, physical anti-terrorism tools, or possibly bomb sniffing dogs.

The provide alert function alerts higher authority in the case of a breach of security or any other anomaly associated with the ECS system.

2. Second-Level Functions

The ECS functional hierarchy continues the flow of functions created from the requirements identified by the stakeholder. This portion of the architecture is an arrangement of functions and their sub-functions and interfaces (internal and external) that defines the execution sequencing, conditions for control or data flow, and the performance requirements to satisfy the requirements baseline (IEEE 1220). Figure 3 shows the second level functional hierarchy for the Automated ECS system. The second level functions that comprise this system of systems are the Command and Control (C2) system, the Detect system, Identify system, and the Alert system.

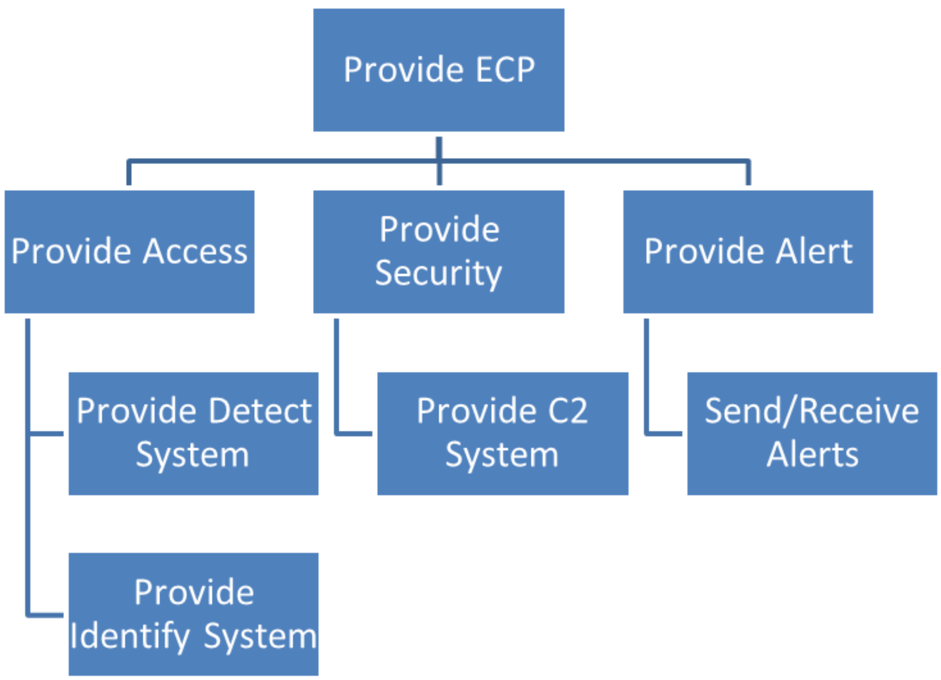

Figure 3. Automated ECS Top-level Functional Hierarchy

The C2 system is a top-down view for the commander or decision maker. All pertinent information is delivered to a viewer(s), usually fed from a server that processes raw data and applies further computations and filters in order to deliver relevant information to the commander. The commander will then have the utility to either query the database for specific analysis or observe the real time operation of the ECS system.

The Detect system is used as a surveillance and facial/license plate recognition system in order to capture images of both the license plate as well as the driver. The facial recognition portion will detect a face in a given picture frame and compare it with a license plate database in order to give probabilities of detection. This system is a bottom-up approach of using sensors to gather raw data for further processing analysis.

The Identify system will contain the database that holds license plate numbers and associated owner/driver information for the respective vehicle. The facial recognition software will reside within this function as well. This function will act as a middleware that takes the raw data from the camera and applies the facial/license plate recognition software in order to determine probability for correct recognition. Anomalies will pass the required information to the Alert system.

The Alert system will take any anomalies and pass the information to the appropriate decision maker. The Alert system will have a minimum threshold for recognition probability. If this threshold is not met, the alert will be forwarded for further analysis.

3. Third-Level Functions

For the purpose of clarity, the figure below displays only the two lowest levels of functions. This final functional decomposition identifies the sub functions that are required of the system in order to accomplish the overall requirements for the automated ECS.

License plates and personnel are intended to be detected from some mix of sensors or cameras located in the vicinity of the automated lane. The Identify system consists of two sub functions: Recognize Face and Provide Database Lookup. Proposed automated systems will provide alternative means of addressing those two sub-functions. The command and control function contains the display and send/receive intelligent data sub functions. Finally, the Alert system will provide notification of either a license plate anomaly or a personnel recognition problem.

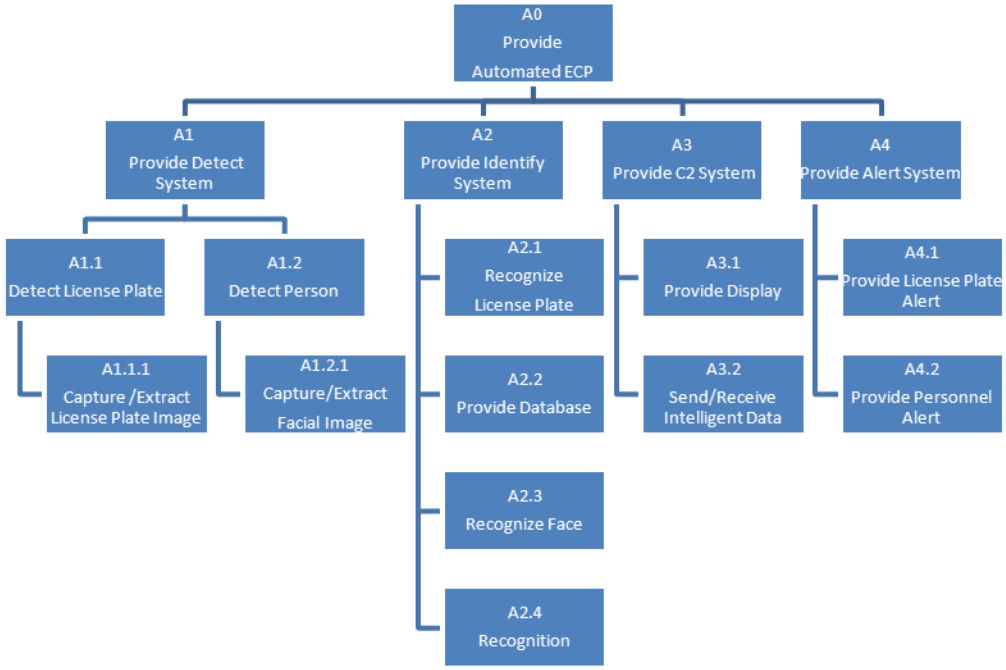

Figure 4. Functional Architecture for Automated ECS system

C. DATA FLOW DECOMPOSITION

Figure 5 shows the data flow decomposition of the top-level function that comprises the automated ECS function. An IDEF 0 figure is used for the standardization of all decomposition figures. The boxes represent the function, the arrows on the left side of the box represent inputs, and the right side is the outputs. The top of the activity box are constraints and the bottom represents the mechanisms by which the action is completed.

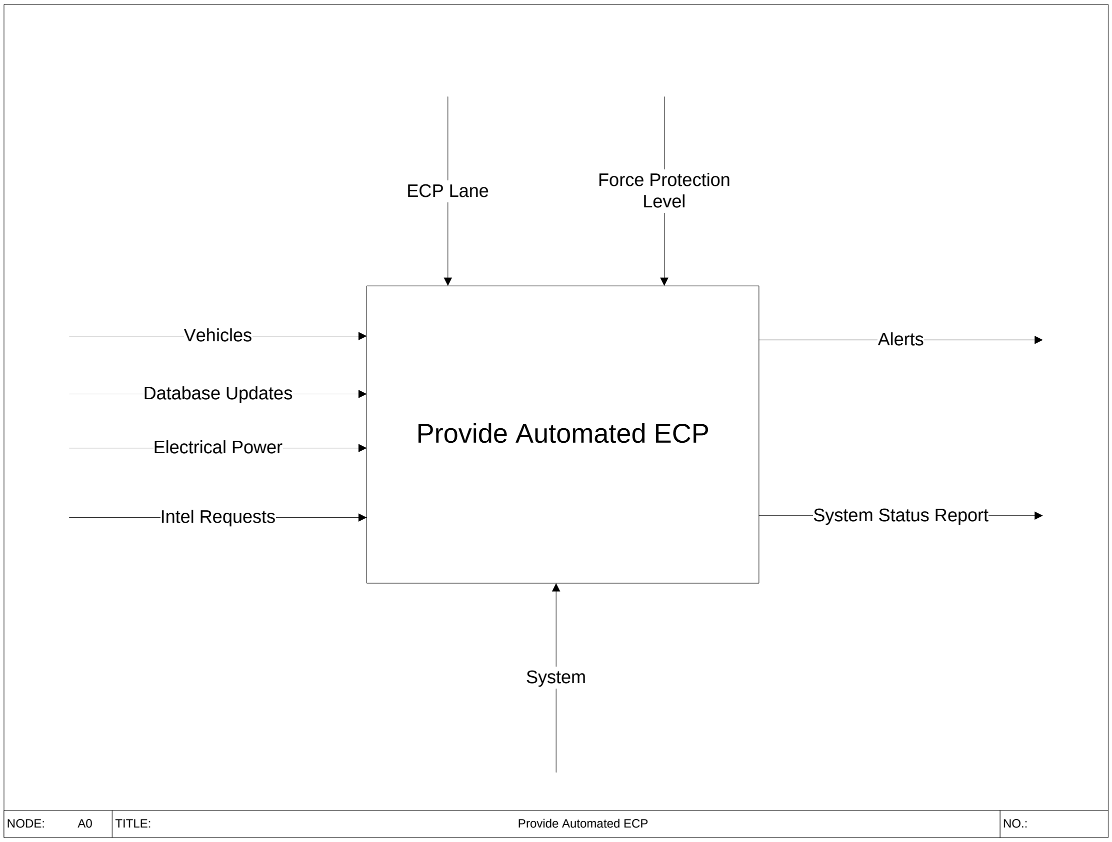

Figure 5. Provide Automated ECS Function

From the top-level decomposition, we can now examine the first level of functions that make up the Provide Automated ECS function. Figure 6 shows this first level of decomposition. The inputs that were provided in Figure 5 can traced into each of the functions.

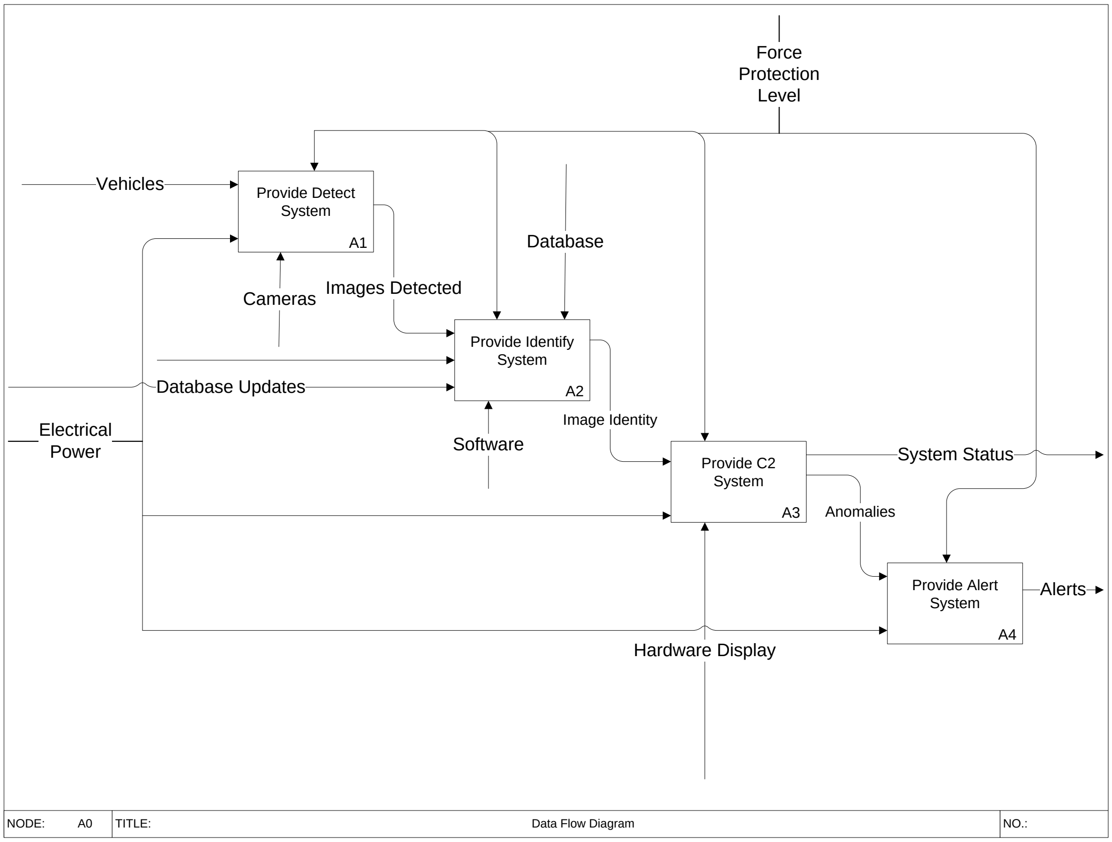

Figure 6. First-Level Data Flow Decomposition

From the first level of data flow decompositions, the detect function will now be examined. Figure 7 shows the decomposition of the Detect function. There are two sub functions that make up the Detect function: Detect license plate and Detect person. The license plate image is captured first and the data is sent to the database and awaits the facial image of the person for later comparison and analysis.

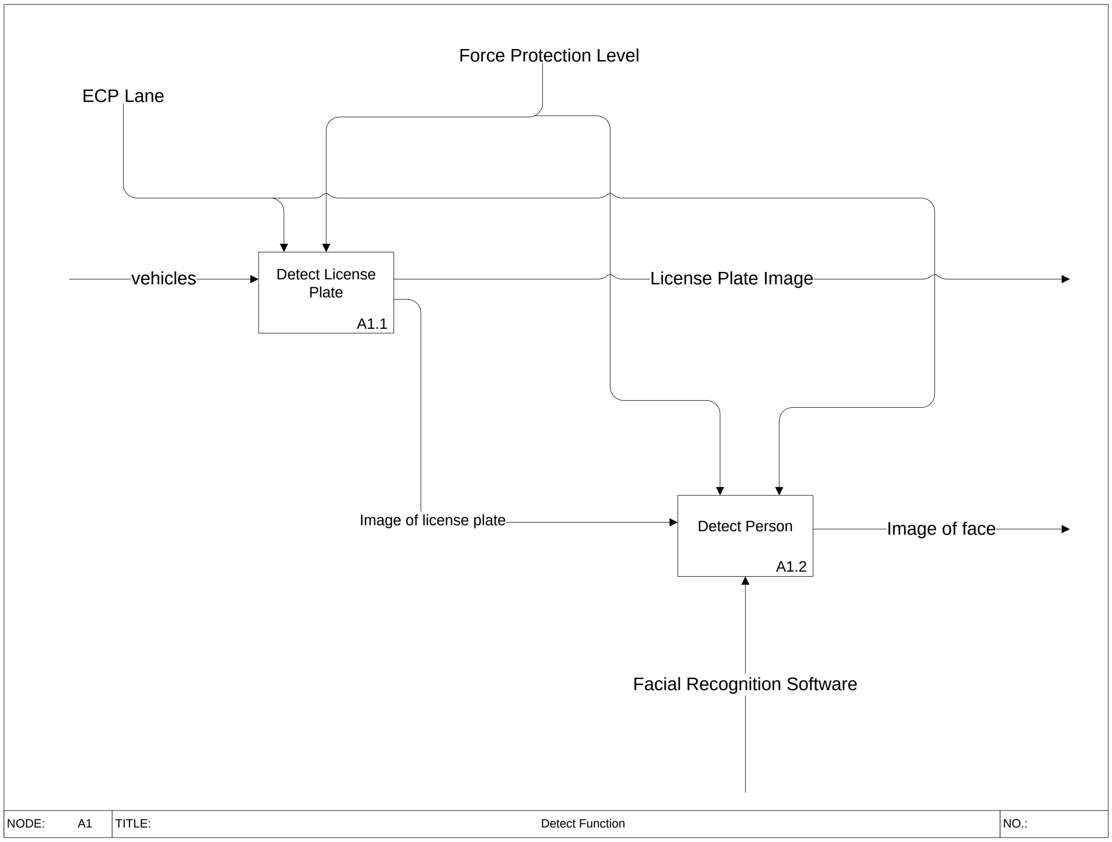

Figure 7. Detect Function Decomposition

Figure 8 decomposes the Identify function. This intricate function will receive the data from the detect system. Namely, the facial and license plate images are sent to the identify function for further analysis. The license plate information is processed and compared against the database for recognition. Once the license plate is found, a picture of the registered driver will accompany the information, which will be used for later comparison of facial features. The facial image is received from the detect function and processed by the Recognize Face sub function. Once this process occurs, the Recognition sub function will compare the database image of the registered driver to the image taken at the automated ECS lane. The Recognition function will output its intelligent data to the Alert and C2 functions.

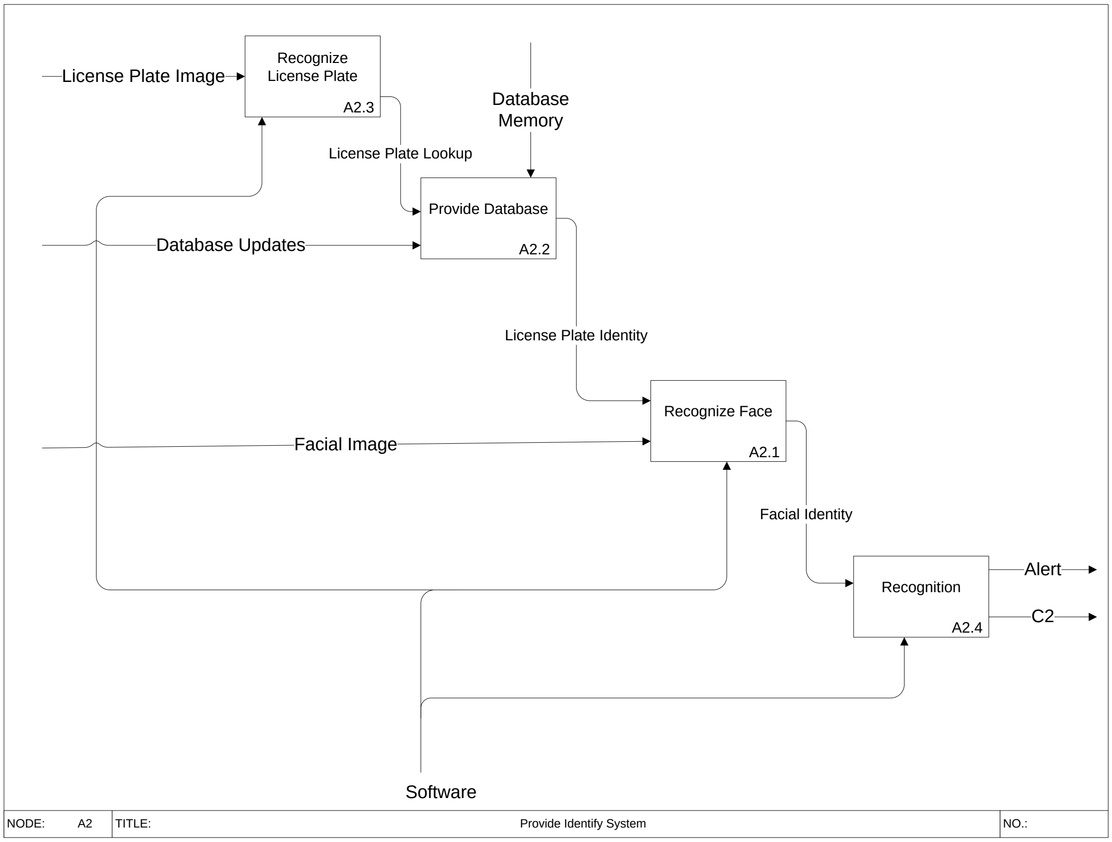

Figure 8. Provide Identify System Decomposition

The Command and Control function allows and interface between the commander and the automated ECS for viewing and query purposes. This function is represented as Figure 9. This function will enable the decision maker to have access to in-depth analysis such as specific vehicle history patterns or trend analysis for traffic prevention.

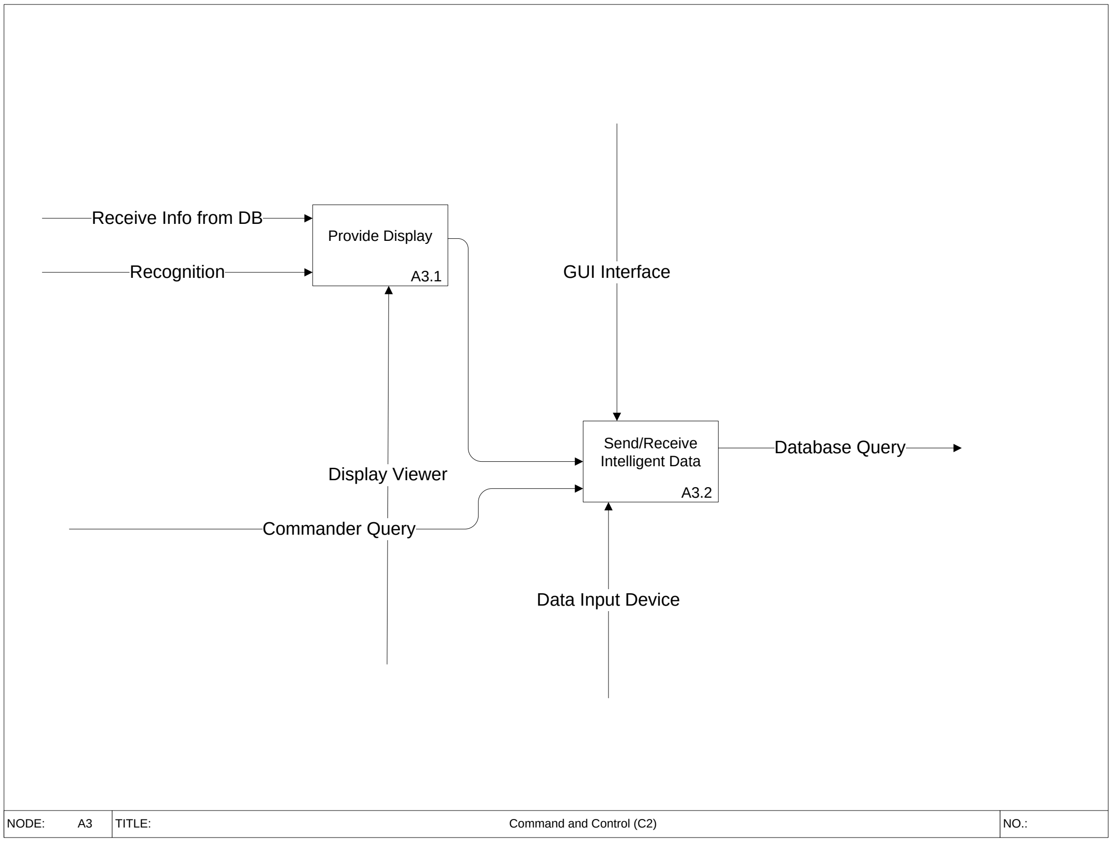

Figure 9. Command and Control Decomposition

The Alert system is shown in Figure 10. This function will provide an alert to the C2 viewer of possible anomalies associated with either the license plate or facial recognition.

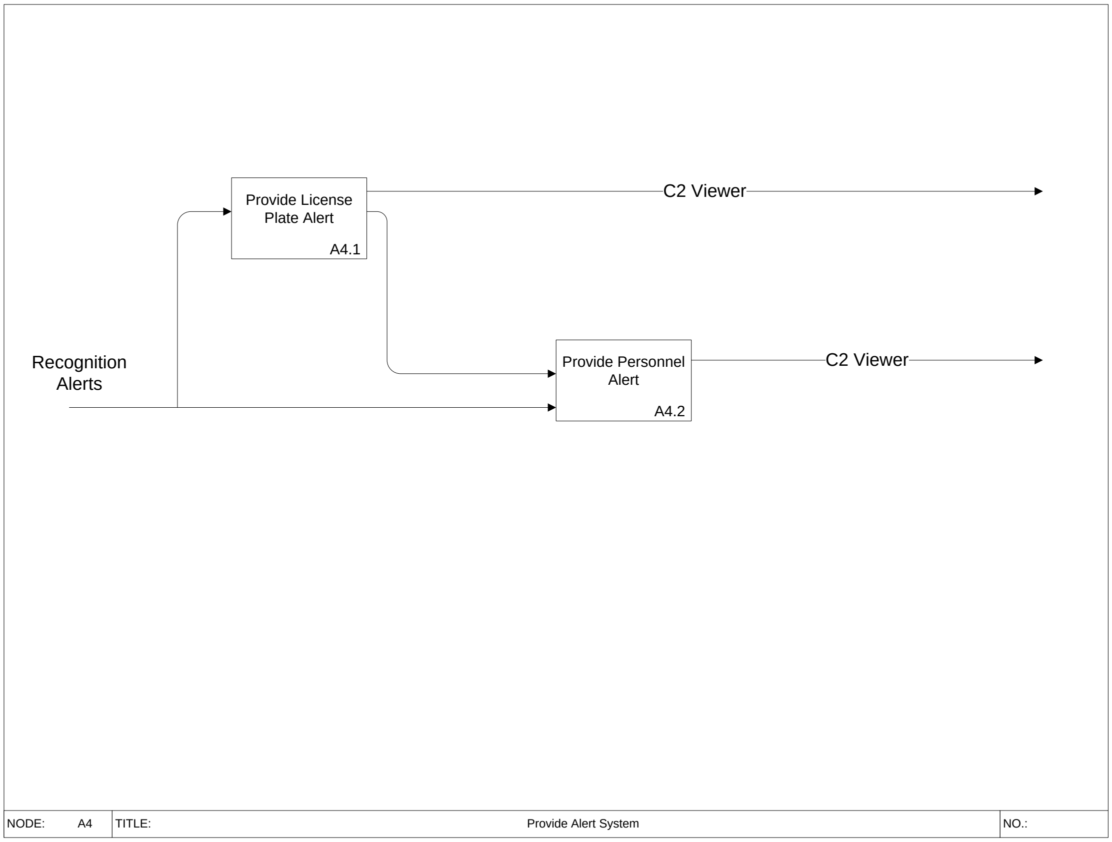

Figure 10. Provide Alert System Decomposition

D. QUALITATIVE VALUE MODEL

A value model is a means to evaluate candidate solutions during the early stages of concept design. This methodology will continue to be refined in the solution design and decision-making phases of the systems decision process (Parnell, Driscoll, and Henderson, 2011). Figure 11 introduces a qualitative value model for the purpose of evaluating the proposed automated ECS system.

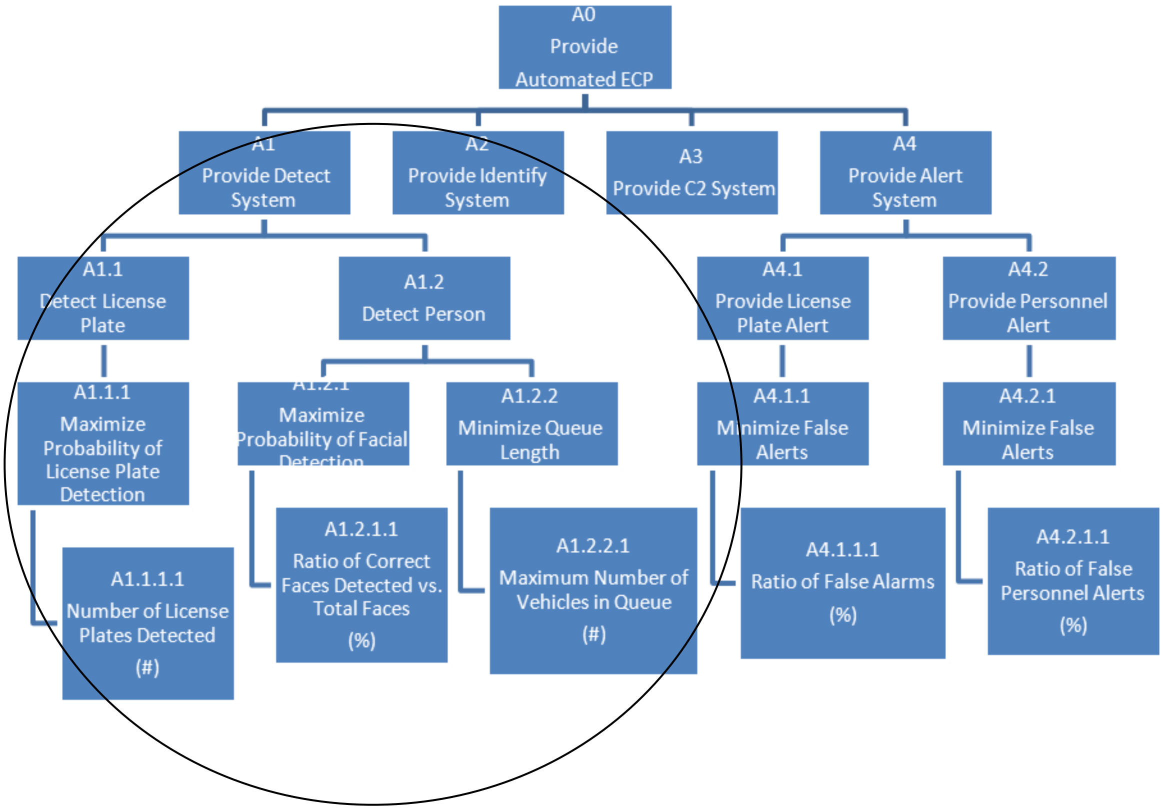

Figure 11. Qualitative Value Model With Emphasis on Detect Function

The qualitative value model presented in Figure 11 presents several objective values for consideration. For purposes of this research, our analysis focuses strictly on the detect function which is represented by the circle in the above figure. The metric, or measure of performance (MOP) used to address the detect function is a ratio of correct recognitions versus the total amount of vehicles. These correct recognitions include both the license plate and the individual driver of the vehicle. Another important aspect will measure the amount of vehicles that are forced to wait in the queue. This portion of the model represents traffic congestion. The maximum number of vehicles that the queue accepts and the amount of time spent in the queue will be evaluated in the model. The impact of false alarms is also an important consideration of this system and while false alarms are not examined as part of this research, they would be important to consider for future work.

E. CONCEPT OF OPERATIONS (CONOPS)

The ECS automated biometric system is similar to the Watchman program with the additional element of license plate recognition. As a vehicle enters the automated lane, a camera will capture the license plate for comparison within the local database. Once the license plate is found, an image of the registered driver of the vehicle will be ready for facial recognition comparison. A second camera will capture an image of the driver as the vehicle approaches the ECS. If a high probability of recognition occurs, the vehicle will be allowed to enter the military installation. If a low probability or anomaly occurs, the vehicle will be directed to a manned kiosk for further investigation conducted by a security guard.

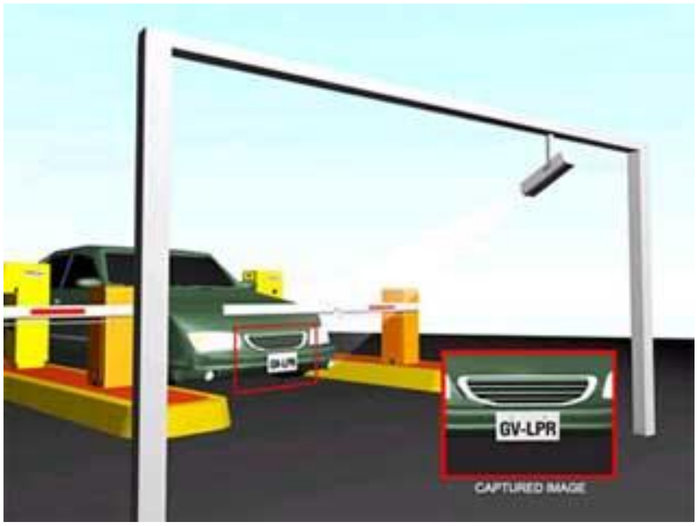

Figure 12. Automated License Plate Recognition Concept

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PHYSICAL ARCHITECTURES

A. ALTERNATIVE GENERATION

Alternative generation ensures that each system function is addressed as part of an overall physical architecture. A morphological analysis or box divides a problem into segments and pairs several solutions for each segment. In the two-dimensional version, a table is created with columns labeled as the functions. Then the elements of each column are filled with competing specific instantiations of each component (Buede, 2000). A morphological box of creating alternatives is presented in Table 1. The baseline operation is color coded in green and the proposed automated ECS is color coded in yellow.

Functions		
Provide Access	**Provide Security**	**Provide Alert**
Manned Access (Baseline)	Use of gate guards, dogs, special equipment	Manual alert to higher authority
Auto Access w/ Facial Recognition	Use auto barricades	Automated alert to higher authority
Auto Access w/ License Plate Recognition	Use automated security measures	
Auto Access w/ LPR and Facial Recognition		

Table 1. Morphological Box of Alternatives

From the above morphological box (Table 1), two alternatives will be utilized in order to compare and contrast the results. The first alternative will be the baseline model. This baseline is currently being utilized at military installations. The second alternative will utilize both the license plate recognition and the facial recognition capabilities.

B. ALTERNATIVE PHYSICAL ARCHITECTURES

Three alternative models will be evaluated in order to provide detailed comparisons for final system determination.

1. Baseline

The baseline architecture will show the capabilities and limitations for the current way that vehicles and personnel are verified at Naval Base San Diego. The ECS has been scaled down in order to get an in depth analysis for how business is currently conducted. All lanes are labor intensive. This means that when a vehicle chooses one of two lanes it is verified and validated by a security guard. Once the security guard is satisfied with the credentials presented, the vehicle and associated personnel are permitted to enter the base.

The other two architectures identified will be a modification from the baseline. Mainly they will consist of combinations of automated ECS lanes as discussed later.

2. Enhanced Architectures

The general architectures that will be presented are derived from the NPS "Watchman" project, an IP-based cameral network system that is able to perform several artificial intelligence systems engineering functions. Five main functions comprise the Watchman system:

1. Personnel Detection and Tracking
2. Behavioral Analysis
3. System Alerts
4. Facial Recognition
5. Automatic Personnel Mustering

This system incorporated Commercial-Off-The-Shelf (COTS) hardware and software technology. The system was open-engineered to enable further development and possibly have applications in base/command security, personnel accountability, and system monitoring (Goshorn, 2010). Similar thesis research explored the possible uses of this Watchman proof of concept applied to Littoral Combat Ships (LCS) and a pier monitoring capability in 2010 by Phil Stubblefield (2010).

From this Watchman theory of operations, the other two alternative architectures are derived. The first alternative implements two fully automated lanes for vehicles to enter. As vehicles are given the opportunity to choose either lane, a vehicle will first go through a license plate recognition system that locates the vehicle from the database. After successful recognition, the vehicle is then required to pass through the facial recognition system. If the automated ECS system correctly recognizes the vehicle and associated driver, they will be permitted to enter the base. The second alternative to the baseline system will use a combination of one manned security guard kiosk and one automated ECS system.

C. LICENSE PLATE RECOGNITION (LPR)

Automated license plate recognition is a COTS technology being utilized by law enforcement around the world. This technology is fast, accurate, and easy to use according to their website disclaimers. The following figure displays a typical LPR configuration. The following illustration shows a typical configuration of a LPR system (for example, for 2-lanes-in and 2-lanes-out access control system). The system ("SeeLane") is a typical example of such system. The SeeLane application runs as a background Windows application in the PC (shown in the center), and interfaces to a set of SeeCarHead camera/illumination units (one for each vehicle) which are interfaced by the frame grabber. The application controls the sensors and controls via an I/O card that is connected thru a terminal block to the inputs and outputs.

The application displays the results and can also send them via serial communication and via DDE messages to other application(s). It writes the information to local database or to optional remote databases via the network (www.licenseplaterecognition.com, accessed May 15, 2011).

Figure 13. Typical 2-Lane LPR Configuration

According to the www.platerecognition.info website, current LPR technology is making vast improvements over previous systems. There are many companies that offer LPR systems and software. Depending on the algorithms used, accuracy is inherently increased or decreased. For standardization purposes, we will evaluate the Finmeccanica Company's MPH-900 Mobile Plate Hunter Advanced LPR system. This system is utilized by over 5,000 law enforcement agencies around the world and can read over 1,800 license plates per minute. The MPH-900 fixed camera system operates in a day or night setting and can identify license plates from all 50 states, Canada, and Mexico. According to the www.elsag.com website, this fixed camera system has a recognition rate above 95%, even at vehicle speeds up to 75 mph (www.elsag.com, accessed May 30, 2011).

Figure 14. MPH-900 Fixed Camera System

D. FACIAL RECOGNITION

The facial recognition technology proposed for this automated ECS system is derived from the NPS "Watchman" program that was detailed in Dr. Deborah Goshorn's Ph.D. dissertation titled, "The Systems Engineering of a Network-Centric Distributed Intelligent System of Systems for Robust Human Behavior Classifications." In this dissertation, a detailed analysis of scenarios, capabilities, and applications are given that describes the Watchman program. Contained in the dissertation is the overall probability for recognition given the parameters used was found to be an average of 90%. Dr. Goshorn uses a "turbocharger" that can increase the probability to 99%. This turbocharger uses a high-level classifier to correct for low-level classification errors (Goshorn, 2010).

E. PROOF OF CONCEPT

A proof of concept is submitted in order to conduct various scenarios, analyze the results, and ultimately recommend a solution to the proposed problem. For the proof of

concept, a discrete event simulation is utilized for this analysis. A simple process flow diagram is shown in Figure 15 that represents the baseline model.

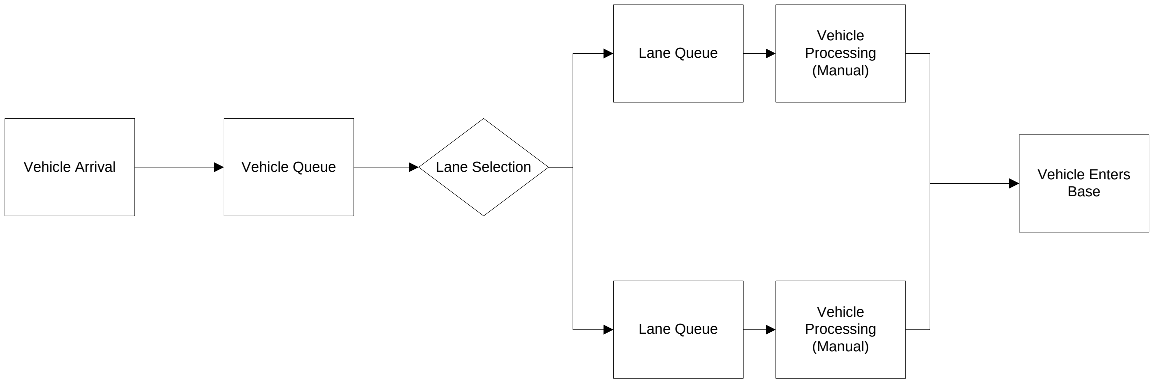

Figure 15. Baseline Representation for Simulation

From Figure 15, vehicles are created based on a set distribution. If the lane queues are either empty or less than the maximum allowance, the vehicle will proceed to one of the two lanes where it will await processing. Once the vehicle and driver are process, the vehicle will enter the military base.

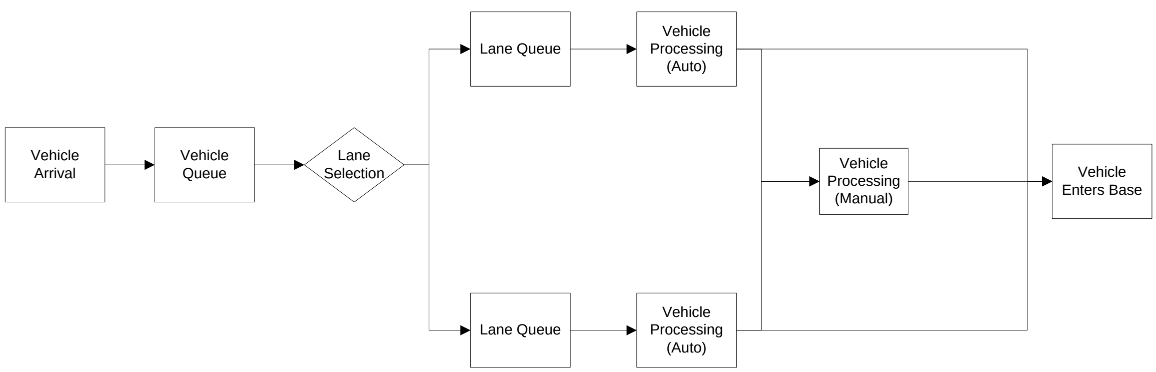

Figure 16. Automated Alternative for Simulation

The first alternative is a fully automated ECS that incorporates two automated vehicle-processing systems that are comprised of a license plate and facial recognition systems. If a vehicle license plate or facial recognition does not match, the vehicle is

diverted to a manual vehicle-processing kiosk for further inquiry. Once a vehicle successfully passes either the automated or the manual processing kiosk, the vehicle is permitted to enter the base.

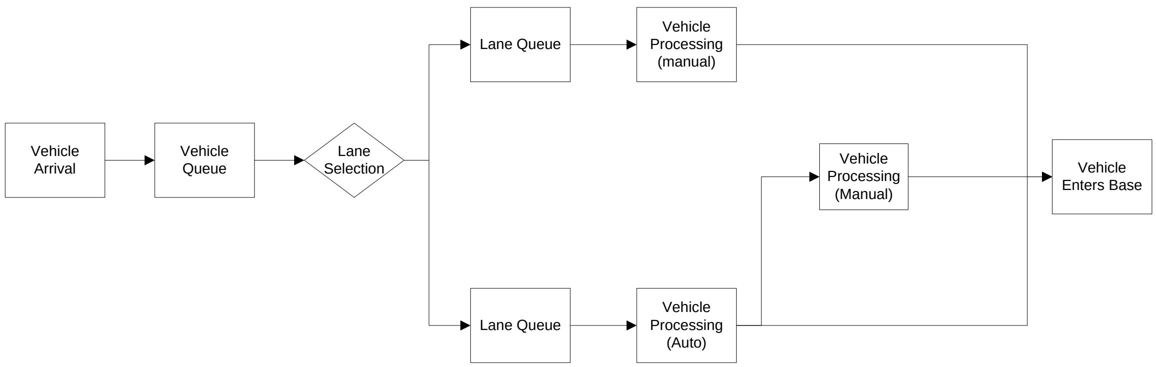

Figure 17. Integrated Auto/Manual Alternative for Simulation

The final alternative integrates both an automated and a manual kiosk system. Figure 17 provides a picture of the configuration used for modeling. Two lanes are utilized however one is automated and one is manual. The automated lane contains a manual kiosk utilized for diverted vehicles that are not recognized. The manual lane provides direct access to the base.

As far as personnel considerations for modeling, the baseline model utilizes two people, one at each manned kiosk. The automated alternative employs one person at the diverted manual kiosk. Finally, the integrated alternative employs two personnel in each of the manned kiosks.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SYSTEM SIMULATION AND ANALYSIS

Before a scenario can be built and modeled, we first have to establish assumptions for standardization purposes. Table 2 shows the assumptions for the model.

Assumptions				
	P(detect)	Throughput (seconds)	Total Vehicles (per Lane)	Duration (minutes)
Baseline	0.99	10	720	120
Automated LPR	0.95	0.03	1440	120
Automated Facial	0.90	5	1440	120

Table 2. Discrete Event Simulation Assumptions

Table 2 lists the assumptions utilized in the discrete event simulation. These assumptions were derived from manufacture specifications and historical or observed data. The baseline system will have a throughput of 10 seconds for each guard station. This means that a vehicle that enters a manual lane will take 10 seconds to be processed once the vehicle reaches the kiosk or guard. Ten seconds is allocated for the guard to properly check the CAC Identification for the driver. Additionally, the security guard must visually inspect the vehicle registration sticker (DoD Form 2220) for possible expiration. If the vehicle stickers are expired, the driver will not be granted access. It is assumed that a guard will maintain 99% detection rate throughout their shift.

For the automated LPR, a throughput of .03 seconds is given based on the reported 1800 cars per minute specification. A probability of detection/recognition of 95% is assumed as well based on claimed specifications. If the license plate is not recognized, the vehicle will be diverted to a baseline guard station for further inquiry.

The automated facial recognition system is assumed to have a throughput of 5 seconds. Once the LPR system recognizes the license plate and a facial image is associated, the facial recognition processing time is estimated at 5 seconds based on the

NPS Watchman characteristics. The probability for correct detection is 90%. This is based on the NPS Watchman scenario results prior to Dr. Goshorn's turbocharger tool.

The following is a list of the assumptions contained within the discrete event simulation:

- Duration – 120 minutes
- Arrival Rate Distribution – Exponential
- Mean Arrival Rate - .02
- All vehicles entering the base are registered and able to use an automated entry lane

Overall, the automated ECS is expected to have at least an 85.5% probability of correct detection per vehicle. This calculation is based on a simple series type circuit. Essentially, one out of every seven cars will need further investigation by a manned guard station.

The duration of the simulation will be 2 hours (120 minutes) in order to represent times between 0600 and 0800. This represents the heaviest time for traffic congestion and when maximum throughput is desired. Total vehicle throughput is limited to 720 per lane with a guard during the two-hour simulation. The number of vehicles is based upon the maximum throughput that a security guard can process and still maintain 99% probability of detection. The automated lane is set to handle 1,440 vehicles. This capacity is based on the 5-second processing time of the facial recognition system.

The arrival rate for the simulation is set to exponential with a mean of .06. The mean value is based on several factors. First, there are approximately 50 ships assigned to Naval Station San Diego. With an average of 300 sailors assigned to each ship, a total of 15,000 sailors are stationed on ships. One third of those ships are usually deployed which brings the total of sailors onboard ships on any given day of the week to be approximately 10,000. I assumed approximately 2,000 sailors and government employees are assigned to San Diego shore billets. Of the 12,000 personnel assigned to Naval Station San Diego, approximately 1/4 of them are in a duty status, which precludes them from requiring access on a given day. This leaves 9,000 personnel that are required to access the naval station each day. The last assumption is that 2/3 of the 9,000

personnel (6,000) will access the entry control points between the hours of 0600 and 0800. With 6,000 people coming to work within a two-hour span, that equals 50 vehicles per minute average. If this is distributed among three access points, a requirement of 2,000-vehicle throughput per ECS is considered a threshold.

A. DISCRETE EVENT SIMULATION CONFIGURATIONS

An Extend Sim discrete event simulation was utilized to model different aspects of an entry control point at a typical military installation.

1. Baseline Simulation

In order to compare and contrast an automated entry control point, we must first establish a baseline. This baseline will model how military bases are commonly accessed today. This system contains two lanes with two guards that check identification and registration requirements. Each lane can hold a maximum of four vehicles before traffic congestion begins and the primary lane starts to backup. The guard spends 10 seconds verifying the information before the car can access the base.

2. Automated Simulation

The automated simulation utilizes two lanes with two automated kiosk stations. Each vehicle enters either of the two lanes and passes through the license plate recognition camera and upon successful recognition is then passed on to the facial recognition system. The entire process is conducted in 5 seconds. If either the LPR or the facial recognition system does not recognize (less than 85% probability of correct recognition) the vehicle/driver, the vehicle is diverted to a manned kiosk for further investigation.

3. Semi-Automated Simulation

With this configuration, one manual and one automated lane is utilized in order to represent an incremental technology introduction.

B. RESULTS

The results of the baseline, automated, and semi-automated discrete event simulations are provided in Table 3.

Simulation Results				
Lane Type	Total Vehicles Created	Total Throughput	Queue Length	Ratio of throughput / total vehicles
Baseline	2065	1438	636	0.696
Automated	1896	1892	1	0.998
Semi Automated	2031	2024	18	0.997

Table 3. Discrete Event Simulation Results

The simulation results given in Table 3 represent the three configurations that were modeled. The baseline configuration yielded the lowest total throughput with 1438 vehicles processed. With the low process rate, we see an increased queue length with equates to traffic congestion. The queue length for the baseline model was 636 vehicles.

The fully automated configuration had a total throughput of 1,892 vehicles and a maximum of 1 vehicle that had to wait in the queue. The semi-automated lane configuration had similar results as the fully automated. All vehicles were processed; however, the queue length was increased slightly to 18 vehicles.

C. ANALYSIS

From the results section, we can see that implementing an automated ECS is the best configuration in order to decrease overall traffic congestion. As predicted, the baseline configuration does not meet the threshold of 2,000-vehicle throughput, which in turn creates traffic and more vehicle congestion. Utilizing a mixed manned and automated control point is the best alternative in terms of better access because of the incremental technology approach. This mitigates the technology risk and still meets the threshold. Overall security using the automated system still needs to be examined.

VI. CONCLUSION AND SUMMARY

A. CONCLUSION

The research that was conducted show great potential for incorporating biometric technology into entry control points. Specifically, through a discrete event simulation I was able to show significant traffic alleviation through maximum vehicle throughput while maintaining high security standards. I showed that overall manning could be reduced without sacrificing access integrity. For incremental technology incorporation, I recommend replacing one manned entry lane and implementing a single automated entry control point to increase vehicle throughput. Once data is collected and any minor automated ECS anomalies are fixed, I recommend implementing a fully automated ECS system.

B. SUMMARY

The Systems Engineering process provided the framework for identifying a capability gap, refining the requirements, decomposing the functions, and ultimately finding a suitable solution. The immediate benefit this technology brings forth is the alleviation of traffic congestion associated with our DoD employees accessing military installations at a common time. By eliminating manning requirements at the manned entry point, that guard would be able to monitor multiple lanes, thus increasing overall situational awareness. The reduction of costs, though not discussed in this thesis, could be easily traced with the reduced manning requirements.

C. FUTURE RESEARCH

Multiple areas exist for further research opportunities. Areas, such as database management, optimization of lanes and technology, also integrating increased security measures, are all areas that need research before implementing an automated entry control point. The previous research of facial recognition from which this thesis draws

upon contains a very small sample size of images. A much larger database of facial images that are associated with many license plate images would need to be tested in order to correctly assess the limitations of facial recognition.

In order to conduct a more complete analysis, future studies should examine the alternative architectures with respect to the remaining functions in the value hierarchy. Additionally, a detailed risk analysis and cost benefit would be beneficial, as well as a closer look at other functional "ilities," such as reliability, maintainability, and human systems integration, or usability.

LIST OF REFERENCES

Advanced Management Program. *Implementing a New Strategy for US Naval Base Functions that Rely on DoD Form 2220 – Vehicle Decals*. Navy Supply Corps School,March 2010. https://www.netc.navy.mil/centers/css/nscs/amp/Presentation/class030/Team_3_pointpaper.pdf

Blanchard, Benjamin, and Wolter Fabrycky. 2006. *Systems Engineering and Analysis*. 4th ed. New Jersey: Pearson Prentice Hall.

Bruce, V. *Understanding Facial Recognition*. British Journal of Psychology. 1990

Buede, Dennis. 2000. *The Engineering Design of Systems Models and Methods*. New York: John Wiley & Sons, Inc.

DTM 09-012. *Interim Policy Guidance for DoD Physical Access Control*. December 8, 2009.

Forsberg, Kevin, Hal Mooz, and Howard Cotterman. 2000. *Visualizing Project Management*. 2nd ed. New York: John Wiley & Sons, Inc.

Goshorn, Deborah. 2010. The Systems Engineering of a Network-Centric Distributed Intelligent System of Systems for Robust Human Behavior Classifications. PhD diss., University of California San Diego.

ELSAG North America. 2011. Accessed on May 30, 2011. http://www.elsag.com

License Plate Recognition. 2008. Accessed on May 15, 2011. http://www.licenseplaterecognition.com

Parnell, Gregory, Patrick Driscoll, and Dale Henderson. 2011. *Decision Making in Systems Engineering and Management.* 2nd ed. New Jersey: John Wiley & Sons, Inc.

Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. Net Centric Attributes List. (2007). http://cio-nii.defense.gov/docs/NetCentricAttributesOfficial.pdf

Stubblefield, Philip. 2010. Security Enhancement of Littoral Combat Ship Class Utilizing an Autonomous Mustering and Pier Monitoring System. Master’s thesis, Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California